

nuclei scanner

- هي اداة موجود جواها templet جاهزه توصلك للثغرات
- جواه اكتر من 8000 templet جاهزه مكتوبه بلغه GO
- خلي بالك ان المواقع بتمنع استخدامها في الغالب
- عشان الاداه دي تاخذ حقها شغلها علي vps برام 64 ويفضل اعلي
- ممكن تستعمل مواقع زي discovery project
- اعمل اميل علي www.digitalocean.com اعمل اكونت هتاخذ 200 دولار منه تاخذ بيهم vps لمدة شهرين

- بتنزلها من github وكمات معاها templet لازم تنزلها عشان تقدر تعمل scan

```
$ ls
cloud          headless      README_KR.md
code          helpers      README.md
CODE_OF_CONDUCT.md http          ssl
Community-Rewards-FAQ.md javascript    templates-checksum.txt
CONTRIBUTING.md LICENSE.md    TEMPLATES-STATS.json
contributors.json network       TEMPLATES-STATS.md
cves.json     passive      TOP-10.md
cves.json-checksum.txt profiles      wappalyzer-mapping.yml
dast          PULL_REQUEST_TEMPLATE.md workflows
dns          README_CN.md
file        README_JA.md
```

- دول ال هتلاقيهم جواه templet
- اهمهم لينا http

```
(kali@kali)-[~/bin/nuclei-templates/http]
$ ls
cnvd          exposures    miscellaneous    token-spray
credential-stuffing fuzzing      misconfiguration vulnerabilities
cves          global-matchers osint
default-logins honeypot     takeovers
exposed-panels iot          technologies
```

```
(kali@kali)-[~/bin/nuclei-templates/http]
$
```

- ودا ال جواها دي الحاجات الي هيدورلك عليها زي cve

تحديد هدف واحد

nuclei -u <https://target.com>

تفعيل كل ال template

nuclei -u <https://target.com> -t مكان تنويع ال /

فحص قائمة URLs من ملف

nuclei -l urls.txt

استخدام template أو مجلد templates

nuclei -u <https://target.com> -t cves/2022/CVE-XXXX.yaml

nuclei -u <https://target.com> -t vulnerabilities/

تحديد مستوى الخطورة

nuclei -u <https://target.com> -severity high,critical

حفظ النتائج في ملف

nuclei -u <https://target.com> -o results.txt

تحديد عدد الطلبات في الثانية

nuclei -u <https://target.com> -rate-limit 20

تمرير الفحص عبر بروكسي

nuclei -u <https://target.com> -proxy <http://127.0.0.1:8080>

إضافة headers مخصصة

nuclei -u <https://target.com> -H "Authorization: Bearer TOKEN"

طباعة النتائج بصيغة JSON

nuclei -u <https://target.com> -json

الوضع التفصيلي verbose

nuclei -u <https://target.com> -vv

تحديث التemplات

nuclei -update-templates

```
root@kali:~# nuclei -u https://testphp.vulnweb.com -o file.txt -mhe  
4
```

- -mhe

- دا بيكون لو عاوز الاداه تبعك لكل موقع عدد معين من الطلبات لان الاداه بتتبعك 30 طلب

```
^C[INF] CTRL+C pressed: Exiting  
[INF] Attempting graceful shutdown...  
[INF] Creating resume file: /root/.cache/nuclei/resume-cr3737uen10vgv  
orqeh0.cfg  
root@kali:~#  
root@kali:~# nuclei -resme
```

- ممكن تستخدم الامر resme لو وقفت الاداه هو بيعملك ملف بالاسم دا اتستخدم الامر ب عشان تكمل scan في وقت ثاني

```
-> nuclei -u https://api.swisscom.com
```

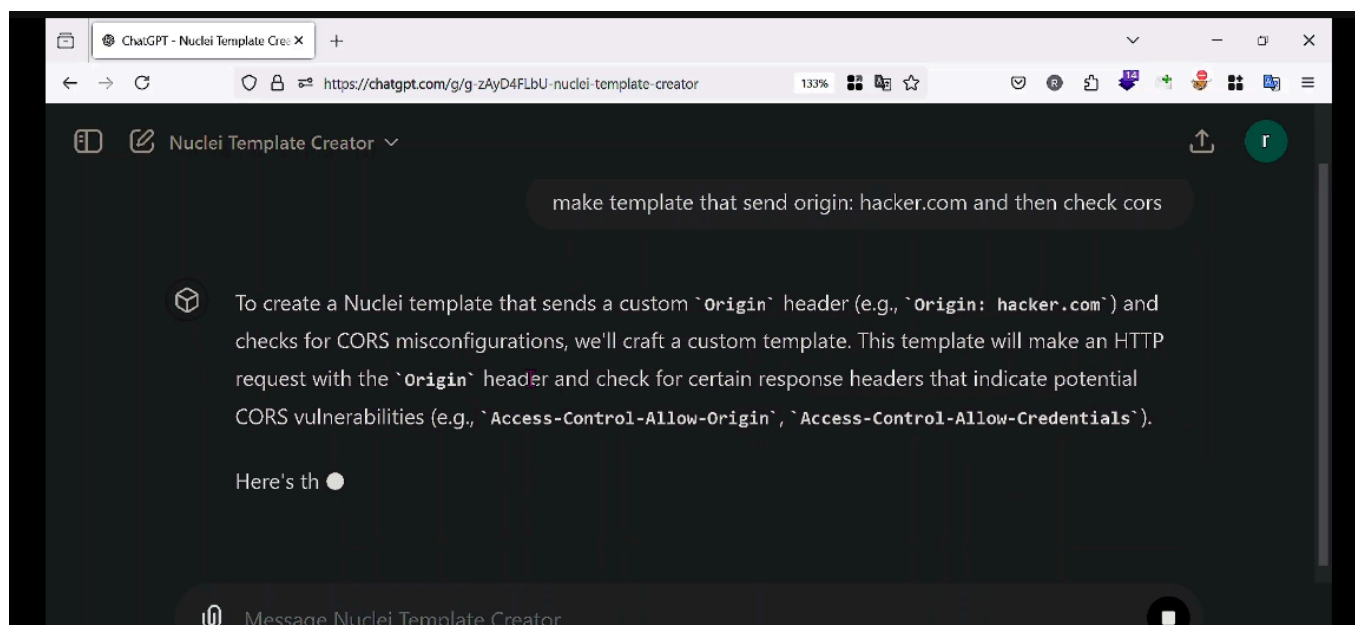
```
=> rate limit => rate limit headers  
- X-Forwarded-For: 127.0.0.1  
- X-Forwarded-Host: 127.0.0.1  
- X-Forwarded: 127.0.0.1  
- Forwarded: 127.0.0.1
```

- ممكن تستعمل اجزاء rate limit عشان ما تاخذش block عن طريق H-

- لو عاوز تعمل templet خاصه بيك

- اول حاجه نت بتقولها نت عاوز يكون اي في الطلب ونت متوقع اي في الرد
- وعلي الاساس دا بتقيس الثغره زي cors مثلا بتحت origin:hacker.com ومستني الرد يكون في

- access-control-allow-origin



- في module كامل في chatgpt يساعدك انك تعمل كذا بكل بسهوله

```
Accept: "../../../../../../../../etc/passwd{t}"
```

- RCE دا ممكن يعملك payload

- عشان تحفظ ال templet بتعمل nano file.yaml
- وتحفظ فيه كل templet ال نت عملتها
- وبعدين تقدر تستعمله عادي مع الاداه عن طريق -t

•